

REMARKS

In the Office Action, claims 1 - 41 were noted as pending in the application, and all claims were rejected. By this amendment, no claims have been amended, added, or canceled. Thus, claims 1 - 41 are pending in the application. The rejections of the Office Action are traversed below.

Rejection of Claims 1 - 5, 10 - 17, 29 - 32, and 37 - 41 under 35 USC §102

In item 4, on pages 2 - 7 of the Office Action, claims 1 - 5, 10 - 17, 29 - 32, and 37 - 41 were rejected under 35 USC §102 as being anticipated by U.S. Patent 5,999,711 to Misra et al. (hereinafter "Misra"). This rejection is respectfully traversed.

The Misra et al. Patent

Misra et al. discloses a method for authenticated connection in a distributed system to machines in a domain other than the home domain (Misra et al. at abstract). Every time a machine is booted within its home domain, it obtains a logon certificate that certifies the identity of the machine and includes authorizations for connecting to the distributed system (Col. 6, lines 45 - 48; Col. 7, lines 8 - 13). Similarly, each time a user logs on to his home domain, he obtains a logon certificate that can be later submitted to provide access to the distributed system (Col. 6, lines 52 - 55; Col. 7, lines 15 - 20).

The Claimed Invention is Patentably Distinguishable Over Misra et al.

The Applicants' claimed invention is directed to a method and system for providing secured access to a resource of a processing system (specification at page 6, lines 11 - 17). The system resource can be an application, transactions, records, and/or equipment (page 6, lines 21 - 31). In particular, and reciting independent claim 1, the claimed method includes the steps of:

establishing a secure communication session between a user desiring access and a logon component of the processing system;

verifying that logon information, provided by the user to the logon component during the secure communication session, matches stored information identifying the user to the

processing system;

- generating a security context from the logon information and authorization information that is necessary for access to the resource;
- providing the security context to the user; and
- sending, by the user to the processing system, the security context and a request for access to the resource.

Advantageously, the user logons to the system once, obtains a security context specifying the user's system resource authorized access rights and proceeds to utilize a variety of system resources transparently to the user and without need for additional logons or security clearances (page 6, lines 18 - 24; page 13, lines 6 - 15; page 23, line 31 - page 24, line 6). In particular, claim 1 recites the feature of establishing a secure communication session between a user desiring access and a logon component of the processing system. From the secure logon session, a security context is generated which the user sends to the processing system for access to a system resource.

In contrast, the system disclosed by Misra et al. is limited to authorizing user access only to remote machines, within a distributed network, that are not part of the user's home domain (Misra et al. at abstract; Col. 5, lines 3 - 6). Accordingly, Misra et al. suffers from the problems disclosed in the present specification at page 1, lines 7 - 23; Fig. 1 wherein a user having access to a system must still provide logon information for each secured system application, i.e., resource, the user desires to access. Furthermore, Misra et al. lacks the streamlined, singular establishing, verifying, and generating steps recited in claim 1 herein for providing a security context sufficient for the processing system to grant access to a system resource. First, Misra et al. requires that both the machine and the user obtain logon certificates (Misra et al. at Col. 5, lines 63 - 64; Col. 6, lines 45 - 58). In contrast, claim 1 herein requires only the user to logon. Then, both the machine and the user must be authorized in the Misra et al. system to access the remote system before access is granted (Misra et al. at Col. 7, lines 6 - 20). Again, claim 1 herein recites a access method without any such limitation. Finally, the user in Misra et al. must logon at least twice before the logon certificate is sent to the desired remote system for access. The first logon is when the user logons to his home domain and obtains a logon certificate (Misra et al. at Col. 6, lines 52 - 57), and the second logon(s) is required for each remote system the user attempts to access

(Misra et al. at Col. 6, lines 57 - 58; Col. 7, lines 6 - 20). Claim 1 recites a single logon step that ultimately concludes with the sending of the security context and access request to the processing system.

The Office Action broadly cites to Col. 1, line 49 - Col. 2, line 21 of Misra et al. as disclosing each of the elements of independent claim 1. The Applicants respectfully submit the Office Action's reliance of the cited portion, or any portion, of Misra et al. is misplaced. The cited portion of Misra et al. merely discloses providing an encrypted secure package of authorization credentials and accessing the secure package for authorization to connect to a distributed system whenever the user sends a request to logon to the distributed system. At the very best, this portion of Misra et al. discloses providing a logon certificate to the user and sending the logon certificate to the remote facility for authenticating user access. Notwithstanding the citations of the Office Action, the cited portion of Misra et al. specifically fails to disclose the recited steps of establishing, verifying, and generating -- all of which occur prior to the step of providing a security context to a user, which is where Misra et al. at Col. 1, line 49 begins.

It is respectfully submitted that Misra et al. fails to disclose each of the features recited in claim 1; and, therefore, Misra et al. cannot reasonably be said to anticipate Applicants' claimed invention. Accordingly, claim 1 is believed to be patentably distinguishable over the Misra et al. document, and it is respectfully requested that the rejection of claim 1 be withdrawn.

Claims 2 - 5 and 10 - 17 depend from claim 1 and include all the features of claim 1 plus additional features which are not taught or suggested by the Misra et al. document. For example, claim 15 specifies the step, after access to the requested resource is granted, of sending a response to the user that includes a request counter that enables the user to match the response to the request for access, which is neither taught nor suggested by Misra et al. The Office Action cites to Misra et al. at Col. 5, lines 46 - 54 as allegedly disclosing this feature. However, the disclosure in Misra et al. at Col. 5, lines 46 - 54 is discussing the content of the logon certificate, is completely silent regarding any request counter, and is presented prior to any access to a requested resource. Therefore, for at least this reason and the reasons set forth above with respect to claim 1, it is submitted that claims 2 - 5 and 10 - 17 patentably distinguish over the Misra et al. document, and withdrawal of the rejection of claims 2 - 5 and 10 - 17 is respectfully requested.

Independent claim 29 recites a processing system having resources that are selectively accessible to users, wherein the processing system includes a logon component that communicates with the communication device and with the information database, wherein the logon component receives logon information provided by the user during a secure communication session, verifies the received logon information by matching against information identifying the user to the processing system that is retrieved from the information database, and generates a security context from the received logon information and authorization information; and wherein the logon component provides the security context to the user's communication device, and the user sends, to the processing system, the security context and a request for access to a resource.

Similar to the features recited in claim 1, independent claim 29 recites a streamlined, singular system for granting access to system resources through a single logon and the generation of a security context from the logon information and authorization information, and sending the security context to the processing system for access to a resource. As discussed above regarding claim 1, not only does Misra et al. fail to disclose such a system, Misra et al. is directed to a much more limited system for accessing remote domains within a distributed system wherein both the machine and the user must successfully logon, and the user must logon at least twice.

Claims 30 - 32 and 37 - 41 depend from claim 29 and include all the features of claim 29 plus additional features which are not taught or suggested by the Misra et al. document. For example, claim 41 specifies that after access to the requested resource is granted, the stateless component sends a response to the user that includes a request counter that enables the user to match the response to the request for access, which is neither taught nor suggested by Misra et al. The Office Action relies on the rejection of claim 1 as support for its rejection of claim 41. However, claim 1 is completely silent regarding a request counter, and the portion of Misra et al. relied upon in the Office Action for rejecting claim 1 is also completely silent regarding such a feature. Therefore, for at least this reason and the reasons set forth above with respect to claim 29, it is submitted that claims 30 - 32 and 37 - 41 patentably distinguish over the Misra et al. document, and withdrawal of the rejection of claims 30 - 32 and 37 - 41 is respectfully requested.

Rejection of Claims 6 - 9, 18 - 28, and 33 - 36 under 35 USC §103

In item 5, on pages 7 - 11 of the Office Action, claims 6 - 9, 18 - 28, and 33 - 36 were rejected under 35 USC § 103 as being unpatentable over U.S. Patent 5,999,711 to Misra et al. in view of Steven M. Bellovin, "Probable Plaintext Cryptanalysis of the IP Security Protocols" (IEEE 1997) (hereinafter "Bellovin"). This rejection is respectfully traversed.

The Bellovin Article

Bellovin discloses the application of the Data Encryption Standard (DES) as used in cipher block chaining mode (CBC) for the encryption of data (Bellovin, page 52, cols 1 - 2).

The Claimed Invention is Patentably Distinguishable Over the Cited Documents

The Applicants' claimed invention is directed to a method of accessing a resource of a processing system. In particular, and reciting relevant portions of independent claim 18, there is disclosed and recited a method of accessing a system resource, including:

providing by a user logon information to a logon component of the processing system during a secure communication session between the user and the processing system;

verifying that the provided logon information matches stored information identifying the user to the processing system;

generating a security context from the logon information and authorization information that is necessary for access to the resource, wherein the security context comprises a plaintext header and an encrypted body; the plaintext header comprises a security context ID, a key handle, and an algorithm identifier and key size; and the encrypted body comprises at least one of a user identifier, an organization identifier, access information, an expiration time, public key information, symmetric key information, and a hash;

providing the security context to the user;

sending, by the user to the processing system, the security context and a request for access to the resource; and

determining, by a stateless component of the processing system, based on the security context sent with the request for access by the user, whether access to the requested resource should be granted to the user.

The Office Action admits on page 7 that Misra et al. fails to disclose a plaintext header, and the Office Action then introduces the Bellovin article to allegedly disclose the plaintext header as recited herein. However, not only does Bellovin fail to remedy the deficiencies of Misra et al. discussed above regarding independent claims 1 and 29, Bellovin also fails to disclose the plaintext header as disclosed and recited herein. In particular, claim 18 recites the security context comprising a plaintext header, wherein the plaintext header includes a security context ID, a key handle, and an algorithm identifier and key size. Both Misra et al. and Bellovin are completely silent regarding these features. Bellovin merely discloses the word, plaintext, as describing information in decrypted form and fails to disclose any of the remaining features recited in claim 18.

Since the combination of Misra et al. and Bellovin fails to disclose every critical element of claim 18, the Office Action has failed to make a prima facie case of obviousness for this claim. Therefore, the Applicants respectfully request the rejection of claim 18 be withdrawn.

While teachings of several documents may be combined to render a claimed invention obvious, there must be a reason, suggestion, or motivation to make the combination. Such a suggestion may come from the references themselves, from certain references known to those skilled in the art, or from the nature of the problem to be solved. The Applicants respectfully assert that no suggestion or motivation exists in either Misra et al. or Bellovin to combine the domain access system of Misra et al. with the plaintext cryptanalysis article of Bellovin to render obvious the resource access method recited in claim 18 herein. Further, the Office Action has failed to cite to any such suggestion or motivation. Instead, the Office Action has asserted, without support, analysis, or citation, that it would have been obvious to modify the combined teachings of Misra et al. and Bellovin with plaintext header. The Applicants respectfully submit that not only is there no motivation in either Misra et al. or Bellovin to support such a combination, but also the Office action has misstated the requirements for supporting a rejection under 35 USC § 103 with a combination of multiple references. The standard for finding a motivation to combine references to allegedly render a claim obvious is a disclosed reason for modifying the teachings of the primary reference (Misra et al.) with the specific teachings (plaintext) of the secondary reference (Bellovin), and not, as asserted in the present Office Action, modifying the combination of the references with an element (plaintext header) that is not found in either reference.

Additionally, for documents to be combined to render a claimed invention obvious, the references must teach in subject matter analogous to that of the invention, which is authenticated access to system resources. Bellovin clearly does not teach in such a subject area, and the Applicants respectfully submit that neither Misra et al. nor Bellovin disclose any suggestion or motivation for the person of ordinary skill in the art of providing authenticated access to system resources to look to the Bellovin article for assistance in solving problems associated with such a system.

For the reasons discussed immediately above, claim 18 is believed to be patentably distinguishable over Misra et al. and Bellovin, whether taken alone or in combination. For this additional reason, it is respectfully requested that the rejection of claim 18 be withdrawn.

Claims 19 - 28 depend from claim 18 and include all the features of claim 18 plus additional features which are not taught or suggested by the Misra et al. or Bellovin documents. For example, claim 27 specifies that at least one of a client time and a request counter is sent by the user to the processing system with the security context and the request for access to the resource, which is neither taught nor suggested by Misra et al. or Bellovin. Therefore, for at least this reason and the reasons set forth above with respect to claim 18, it is submitted that claims 19 - 28 patentably distinguish over the Misra et al. and Bellovin documents, whether taken alone or in combination, and withdrawal of the rejection of claims 19 - 28 is respectfully requested.

Claims 6 - 9 depend from claim 1 and include all the features of that claim plus additional features. Therefore, for at least the reasons set forth above with respect to claim 1, it is submitted that claims 6 - 9 patentably distinguish over the Misra et al. and Bellovin documents, whether taken alone or in combination, and withdrawal of the rejection of claims 6 - 9 is respectfully requested.

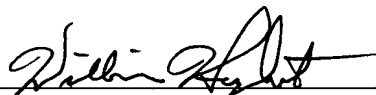
Claims 33 - 36 depend from claim 29 and include all the features of that claim plus additional features. Therefore, for at least the reasons set forth above with respect to claim 29, it is submitted that claims 33 - 36 patentably distinguish over the Misra et al. and Bellovin documents, whether taken alone or in combination, and withdrawal of the rejection of claims 33 - 36 is respectfully requested.

Summary

It is submitted that none of the documents, either taken alone or in combination, teach the claimed invention. Thus, claims 1 - 41 are deemed to be in a condition suitable for allowance. Reconsideration of the claims and an early Notice of Allowance are earnestly solicited. If any fees are required in connection with this Amendment, please charge the same to our Deposit Account No. 02-4800.

Respectfully submitted,

Burns, Doane, Swecker & Mathis, L.L.P.

By: 
William N. Hugnet
Reg. No. 44,481

P.O. Box 1404
Alexandria, Virginia 22314-0404
Telephone: (703) 836-6620
Facsimile: (703) 836-2021

Date: December 6, 2004

VA 587667.1